R E P U B L I Q U E F R A N Ç A I S

PCT/EP2004/012532
07.12.04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

EP04/12532

REC'D 17 DEC 2004
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 15 NOV. 2004

Pour le Directeur général de l'Institut national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

FR/EP2004 017532
07.12.04

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE
page 1/2

R1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /300301

Réservé à l'INPI

REMISE DES PIÈCES DATE 17 NOV 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0313417
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 17 NOV. 2003

Vos références pour ce dossier *(facultatif)* BLO/FC-BFF030417

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET PLASSERAUD
65/67, rue de la Victoire
75440 PARIS CEDEX 09

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE POUR EFFECTUER UN CONTROLE DE SECURITE DES FLUX DE DONNEES ECHANGEES ENTRE UN MODULE ET UN RESEAU DE COMMUNICATION, ET MODULE DE COMMUNICATION

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°
☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale		NORTEL NETWORKS LIMITED
Prénoms		
Forme juridique		
N° SIREN		
Code APE-NAF		
Adresse	Rue	2351 Boulevard Alfred Nobel St.LAURENT, QUEBEC H4S2A9
	Code postal et ville	
	Pays	CANADA
Nationalité		Canadienne
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

R2

Réservé à l'INPI

REMISE DES PIÈCES 17 NOV 2003
DATE
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT 0313417
NATIONAL ATTRIBUÉ PAR L'INPI

DB 540 W /300301

Vos références pour ce dossier : *(facultatif)*		BLO/FC-BFF030417
6 MANDATAIRE		
Nom		
Prénom		
Cabinet ou Société		CABINET PLASSERAUD
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	65/67 rue de la Victoire
	Code postal et ville	75009 PARIS FRANCE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Bertrand LOISEL
CPI n° 94-0311

VISA DE LA PRÉFECTURE OU DE L'INPI

L. MARIELLO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE POUR EFFECTUER UN CONTROLE DE SECURITE DES FLUX DE DONNEES ECHANGEES ENTRE UN MODULE ET UN RESEAU DE COMMUNICATION, ET MODULE DE COMMUNICATION

La présente invention concerne les systèmes de communication, et en particulier les modules de communication.

L'invention trouve application dans le domaine des systèmes de communication dans lesquels un service d'échange de données est fourni. Elle s'applique en outre particulièrement bien à des systèmes de radiocommunication qui offrent un service d'échanges de données tels que le GPRS (« General Packet Radio Service ») ou l'UMTS ("Universal Mobile Telecommunication System"), et de préférence dans les terminaux de radiocommunications de ces systèmes.

Les réseaux IP (« Internet Protocol ») ou X.25 sont des exemples de réseaux d'échange de paquets, communément appelés réseaux PDN (de l'anglais « packet data network »). Chaque élément de réseau d'un réseau de paquet est usuellement muni d'un contrôleur de transmission et de réception de paquets échangés conformément à un protocole d'échange de paquets (PDP, ou « packet data protocol ») donné. Il est fréquent de doter le contrôleur de certains éléments de réseau d'un système dit garde-barrière, ou pare-feu (en anglais « firewall »), dont la fonction est de protéger l'élément de réseau par le biais d'un contrôle sur les flux de paquets transmis ou reçus par l'élément de réseau. Le système pare-feu filtre les paquets en réception, et contrôle aussi l'émission des paquets en transmission. Ce système est fréquemment implémenté dans un module logiciel qui coopère avec le contrôleur de transmission et de réception des paquets.

L'article « Network Firewalls », publié en septembre 1994 par S.M. Bellovin et W. R. Cheswick dans le magazine « IEEE Communications Magazine » fournit une description détaillée des pare-feux et des technologies afférentes.

La structure classique d'un pare-feu est illustrée à la figure 1. Deux filtres 1,2 entourent une ou plusieurs passerelles 3. Chaque filtre 1,2 a pour fonction d'analyser et de contrôler de manière unidirectionnelle ou

bidirectionnelle les flux de paquets échangés sur les liens 4 et 5. Un filtre est ainsi amené à rejeter un paquet, le laisser passer ou bien l'ignorer, et ce sur la base de critères de filtrage. La passerelle ou le groupe de passerelles 3 a pour fonction d'exercer un contrôle applicatif sur les flux de données que le filtre placé en amont laisse passer. Les règles de contrôle et critères de filtrage sont définis et configurables au moyen d'un module 6 de configuration relié à chacun des composants 1, 2, 3 du pare-feu.

Les critères de filtrage peuvent par exemple, de manière connue en soi, être définis sur la base de l'adresse source ou de destination, ou bien du service source ou destination des paquets à filtrer. Dans le cas d'un pare-feu opérant sur des paquets TCP/IP ou UDP/IP, il peut s'agir de l'adresse IP source ou de destination d'un datagramme, ou bien du port UDP ou TCP source ou de destination d'un paquet UDP ou TCP. Ainsi, un filtre 1, 2 peut être configuré de manière à ne laisser passer que les paquets TCP à destination d'un numéro de port donné, correspondant à un service déterminé.

La passerelle ou le groupe de passerelles 3 effectue un contrôle relativement à un ou plusieurs critères relatifs à une application donnée. Un exemple typique consiste, dans le cas d'une application d'échange de courriers électroniques, en un filtrage applicatif des courriers échangés sur la base par exemple d'informations qui sont repérées dans l'en-tête ou le corps d'un message de courrier.

En général, le filtre 1 est bidirectionnel et configuré de manière à protéger les équipements en aval, parmi lesquels se trouvent les passerelles 3, le filtre 2 et les équipements reliés au lien 5, et agit sur les flux de données échangés sur le lien 4. Le filtre 2, lui aussi bidirectionnel, fournit un rempart supplémentaire pour protéger les équipements reliés au lien 5.

Bien souvent des nœuds de réseau tels que des passerelles, des routeurs, ou des ponts sont dotés d'un pare-feu. Cela permet notamment d'isoler un réseau privé (par exemple un réseau d'entreprise, ou un intranet) d'un réseau public (typiquement le réseau Internet) auquel il est relié. Les pare-feux sont ainsi largement utilisés dans le contexte des réseaux interconnectés.

Ils le sont aussi dans celui des ordinateurs personnels dotés des moyens logiciels et matériels pour se connecter au réseau Internet, directement ou par l'intermédiaire d'un fournisseur de service Internet (en anglais ISP, pour « Internet Service Provider »). Un usager peut ainsi doter son ordinateur personnel d'un logiciel pare-feu afin de le protéger lors des connexions au réseau Internet.

De fait, il peut être envisagé de doter tout système capable d'échanger des données avec un réseau de communication de données d'un pare-feu tel que celui décrit à la figure 1. C'est ce qui est fait dans la demande internationale WO 03/017705, qui divulgue l'intégration d'une pluralité d'applications logicielles au sein d'un terminal de radiocommunication, parmi lesquelles une application pare-feu qui coopère avec une unité de filtrage de paquets.

La demande EP 1 094 682 divulgue par ailleurs un téléphone mobile ou une unité d'accès mobile pour communiquer avec un réseau d'échange de paquets qui comprend une fonction de sécurité, assurée par exemple par une passerelle de sécurité.

L'utilisation des pare-feux dans le contexte des réseaux de radiocommunications a aussi fait l'objet d'un article, intitulé « Firewalls for Security in Wireless Networks » (Murthy et al., Proceedings of the Thirty-First Hawaii International Conference on System Sciences, 1998, Volume: 7 , 6-9 Jan. 1998) dans lequel les auteurs décrivent un système dans lequel un pare-feu est mis en œuvre au sein de l'infrastructure d'un réseau de radiocommunication.

L'inconvénient majeur des solutions proposées est qu'elles ne permettent pas la mise en œuvre d'une fonction de sécurité au sein d'une station mobile adaptée à la diversité des réseaux de communication avec lesquels une station mobile est aujourd'hui susceptible d'échanger des données. Elles ne proposent en effet que des fonctions de sécurité qui agissent sans distinction sur l'ensemble des flux de données échangés par une station mobile. Ce problème, qui n'est pas spécifique aux systèmes de

radiocommunications, se pose également dans le contexte plus global de la mise en œuvre d'une fonction de sécurité au sein d'un équipement de communication susceptible d'échanger simultanément des données avec des réseaux de communication qui soit adaptée à la diversité des conditions de sécurité souhaitables lors d'un échange de données avec chacun de ces réseaux.

Le but de la présente invention est de proposer une nouvelle architecture optimale de la fonction de sécurité au sein d'un équipement de communication ne présentant pas les inconvénients exposés ci-dessus.

L'invention propose ainsi un module de communication comprenant des moyens pour échanger des flux de données avec un réseau de communication dans le cadre de sessions de communication établies et organisées selon des contextes de session de communication, et des moyens de sécurité pour contrôler les flux de données échangés. Les moyens de sécurité pour contrôler les flux de données échangés sont agencés pour opérer relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

Les moyens de sécurité pour contrôler les flux de données échangés selon l'invention remplissent une fonction de sécurité, agencée au sein d'un module de communication, qui agit dans le cadre d'une session de communication, et ce par le biais du contexte de session de communication associé. Cette solution permet la mise en œuvre d'une fonction de sécurité dans un cadre plus spécifique que celui du simple échange de données.

Selon l'invention, les moyens de sécurité pour contrôler les flux de données échangés peuvent être agencés pour opérer relativement à un identifiant du contexte de session de communication de la session correspondante, et/ou à un paramètre constitutif dudit contexte. Des exemples de paramètres utilisables dans le cadre de l'invention sont une adresse qui peut être celle du module selon l'invention ou d'un équipement au sein duquel il est incorporé, la qualité de service associée à l'échange de flux de données, ou bien l'identifiant d'un réseau cible.

De manière avantageuse, les moyens pour échanger des flux de données comprennent des moyens pour échanger des flux de données en paquets, et les moyens de sécurité pour contrôler les flux de données sont agencés pour opérer sur des données en paquets.

Plus spécifiquement, les moyens de sécurité pour contrôler les flux de données échangés peuvent être structurés sur la base de la structure classique d'un pare-feu décrite précédemment. Ils peuvent ainsi comprendre un filtre pour opérer par filtrage des flux de données relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

Les moyens de sécurité pour contrôler les flux de données échangés peuvent de manière alternative, comprendre un premier et un second filtres pour opérer par filtrage des flux de données échangés, et une ou plusieurs passerelles pour contrôler les flux de données échangées relativement à un ou plusieurs critères relatifs à une application donnée, l'un au moins des premier et second filtres étant alors agencé pour opérer relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

L'invention trouve une application particulièrement avantageuse dans le domaine des radiocommunications. Il est ainsi prévu d'intégrer le module selon l'invention dans un module de radiocommunication, ou un équipement d'infrastructure de radiocommunication. De manière typique, le module de radiocommunication sera incorporé dans une station mobile.

L'invention prévoit en outre un procédé pour effectuer un contrôle de sécurité des flux de données échangés entre un module de communication et un réseau de communication dans des sessions de communication organisées selon des contextes de session de communication, dans lequel on établit une session de communication avec un correspondant distant, suivant un contexte de session de communication actif, et on contrôle les flux de données échangées selon le contexte de session de communication activé, relativement à au moins un paramètre attaché audit contexte. De manière avantageuse, ce

procédé sera appliqué à des flux de données en paquets.

Selon l'invention, le contrôle des flux de données échangés peut opérer relativement à un identifiant du contexte de session de communication de la session correspondante, et/ou à un paramètre constitutif dudit contexte.

On pourra aussi envisager de contrôler les flux de données échangées selon le contexte de session de communication actif conformément au procédé selon l'invention en filtrant lesdits flux de données au moyen d'un filtre qui opère relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

De manière alternative, l'étape de contrôle des flux de données échangés selon le contexte de session de communication actif pourra être mise en œuvre en filtrant lesdits flux de données au moyen d'un premier et d'un second filtres pour filtrer les flux de données échangés, et d'une ou plusieurs passerelles pour contrôler les flux de données échangées relativement à un ou plusieurs critères relatifs à une application donnée, l'un au moins des premier et second filtres étant agencé pour opérer relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

L'invention propose enfin un programme d'ordinateur chargeable dans une mémoire associée à un processeur, et comprenant des instructions pour la mise en œuvre d'un procédé tel que défini ci-dessus lors de l'exécution dudit programme par le processeur, ainsi qu'un support informatique sur lequel est enregistré ledit programme.

D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels:

- la figure 1 est un schéma synoptique de la structure classique d'un pare-feu ;

- la figure 2 est un schéma illustrant un système de communication comprenant une station mobile incorporant un module selon l'invention ; et
- la figure 3 illustre un exemple d'architecture du module selon l'invention.

L'invention sera dans la suite décrite dans le cadre non limitatif des systèmes de radiocommunication qui fournissent un exemple particulièrement pertinent de sa mise en œuvre.

La figure 2 illustre la mise en œuvre de l'invention au sein d'une station mobile 21 en communication avec deux réseaux 24, 25, dont l'un est un réseau public et l'autre est un réseau privé.

Les communications, en particulier les échanges de données, s'effectuent par le biais d'un réseau de radiocommunication, par exemple un réseau cellulaire à couverture étendue (PLMN) (« Public Land Mobile Network »). Ce PLMN est classiquement divisé en un cœur de réseau 23, comprenant des commutateurs interconnectés, et un réseau d'accès radio (RAN) (« Radio Access Network ») 22 fournissant les liens radio avec les stations mobiles 21.

Dans l'exemple représenté, le PLMN est de seconde génération et de type GSM. Il incorpore dans ce cas un service de transmission de paquets de type GPRS (« General Packet Radio Service »). Dans le GSM, le réseau d'accès 22, appelé BSS (« Base Station Sub-system »), se compose de stations de base (BTS) distribuées sur la zone de couverture du réseau pour communiquer par radio (interface Um) avec les stations mobiles 21, et de contrôleurs de stations de base (BSC) reliés au cœur de réseau 23 et supervisant chacune des stations de base à travers des interfaces appelées Abis. Les protocoles utilisés dans le PLMN GPRS sont décrits dans les spécifications techniques GSM 23.060 (version 5.6.0, Release 5, juillet 2003), 03.64 (version 8.9.0, Release 1999, novembre 2002), 08.16 (version 8.0.1, Release 1999, juillet 2002) et 29.061 (version 5.7.0, Release 5, octobre 2003) publiées par le 3GPP.

L'invention est applicable à d'autres types de PLMN, notamment à des réseaux de troisième génération de type UMTS (« Universal Mobile Telecommunications System ») ou CDMA 2000.

Le cœur de réseau dans la norme UMTS comprend deux domaines distincts correspondant à un découpage entre les services à commutation de circuit (CS, pour « Circuit Switched ») et ceux à commutation de paquets (« PS, pour « Packet Switched »). On distingue ainsi le domaine PS (« Packet Switched Domain ») du domaine CS (« Circuit Switched Domain »). Certaines fonctions, comme notamment l'établissement d'appel, sont ainsi gérées différemment, et réalisées dans des équipements du cœur de réseau différents selon qu'elles sont réalisées dans l'un ou l'autre de ces deux domaines.

Le cœur de réseau 23 est relié au réseau d'accès radio 22 au moyen d'une interface, appelée interface A, Gb pour le GSM, et Iu, pour l'UMTS.

Le cœur de réseau 23 est en outre relié à des réseaux fixes comportant un ou plusieurs réseaux de transmission de données en paquets utilisant des protocoles respectifs (PDP) tels que X.25 ou IP. Dans l'exemple illustré par les dessins, il y a un réseau public de transmission de paquets 25 constitué par le réseau Internet, et un réseau privé de transmission de paquets 24 constitué par un réseau Intranet.

Le cœur de réseau 23 comporte pour le mode paquets des commutateurs appelés GSN (« GPRS Support Node »), qui communiquent entre eux à travers une interface appelée Gn. Les commutateurs de paquets reliés aux BSC du réseau d'accès 22 sont appelés SGSN (« Serving GSN »), tandis que d'autres commutateurs de paquets, appelés GGSN (« Gateway GSN »), servent de passerelle avec les réseaux de paquets, notamment le réseau Internet 25 et le réseau Intranet 24. Ces passerelles sont reliées aux SGSN pour permettre aux stations mobiles 21 d'accéder aux réseaux 24, 25.

La procédure d'établissement d'appel dans le domaine PS de l'UMTS ou dans le réseau de commutation de paquets GPRS fait intervenir la notion de contexte PDP. Un contexte PDP est un exemple particulier de contexte de

session de communication, que l'on peut définir comme un ensemble d'informations relatives à une session de communication.

La notion de contexte PDP est décrite au paragraphe 7.2.1 de l'ouvrage de référence de P. Lescuyer : « UMTS, Les origines, L'architecture, La norme » (2ème édition, Dunod, 2002). Le contexte PDP regroupe l'ensemble des informations permettant la transmission des données usager entre le mobile, le réseau UMTS et le réseau de commutation de paquets externe (par exemple Internet).

Avant d'initier tout transfert de données, la station mobile 21 doit nécessairement demander au cœur de réseau 23 l'activation d'un contexte PDP, qui devra vérifier la conformité des attributs du contexte demandé par rapport aux caractéristiques de l'abonnement souscrit par l'usager.

Plusieurs contextes PDP peuvent être actifs simultanément pour un usager donné. L'usager peut en effet vouloir activer plusieurs sessions en parallèle, par exemple pour relever simultanément deux boîtes aux lettres électroniques détenues par deux fournisseurs de services différents. Dans ce cas, le mobile doit activer autant de contextes PDP que de sessions. Grâce à cette fonctionnalité, un utilisateur peut en théorie à la fois naviguer sur l'Internet en utilisant le protocole WAP (« Wireless Application Protocol ») sur son téléphone portable GPRS et consulter un site Web sur son ordinateur connecté à son téléphone portable, via l'activation de deux contextes PDP.

Deux contextes de session de communication 26, 27 ont été activés au sein de la station mobile 21. Dans l'exemple illustré par les dessins, il s'agit de deux contextes PDP actifs. Chaque contexte PDP est relatif au réseau avec lequel on souhaite initier une session de communication, et la station mobile 21 a une session de communication active avec le réseau intranet 24, et deux sessions de communication actives avec le réseau public Internet 25.

La procédure d'activation d'un contexte PDP par une station mobile est décrite en détails au paragraphe 9.2.2.1 de la spécification 3GPP TS 23.060.

Pour initier cette procédure, la station mobile envoie un message

d'activation ACTIVATE PDP CONTEXT REQUEST au SGSN. Ce message indique les valeurs des différents paramètres du contexte PDP dont on requiert l'établissement, dont les principaux sont :

- l'adresse PDP de la station mobile 21. Dans le cas d'un réseau externe Internet, il s'agit d'une adresse IP v4 ou IP v6. Pour chaque contexte PDP 26, 27 en cours, la station mobile se voit donc attribuer une adresse IP temporaire ;
- la qualité de service associée à la communication, qui est représentée par les attributs du lien radio alloué par le réseau d'accès 22 ;
- l'APN (« Access Point Name), qui correspond à l'identifiant du réseau fixe 24, 25 auquel le mobile souhaite accéder.

Comme indiqué précédemment, plusieurs contextes PDP peuvent être actifs simultanément, de sorte qu'une station mobile pourra simultanément avoir plusieurs adresses PDP - typiquement plusieurs adresses IP source - distinctes. L'invention permet alors par exemple la mise en œuvre d'une fonction de sécurité qui opère de façon indépendante sur chacun des flux échangés avec ces adresses IP source multiples.

Selon l'invention, l'activation de chaque contexte de session de communication 26, 27 – dans l'exemple illustré chaque contexte PDP - donne lieu à la création d'une tâche logicielle de sécurité 28, 29 qui fournit les fonctions d'un pare-feu telles que précédemment décrites, et opère dans le cadre des échanges effectués selon le contexte 26, 27 auquel elle est associée. Chaque tâche logicielle de sécurité 28, 29 est en effet susceptible d'effectuer une opération sur les flux de données échangées dans le cadre d'une session de communication définie dans le contexte 26, 27 correspondant. Par exemple, des paramètres de filtrage en fonction des adresses IP et/ou des ports TCP ou UDP des datagrammes reçus ou envoyés diffèreront selon qu'il s'agit du contexte 26 de communication avec le réseau Intranet 24, ou du contexte 27 de communication avec le réseau Internet 25. On pourra notamment souhaiter de paramétrer la tâche logicielle de sécurité 28 de manière à fournir une sécurité accrue pour l'accès à l'Internet public – ce qui

se traduira par des paramètres de filtrage actif plus restrictifs – par rapport au paramétrage de la tâche logicielle de sécurité 29 pour l'accès à l'Intranet, de manière à ne pas gêner éventuellement l'exécution des applications propres à ce réseau privé qui offre par nature une meilleure sécurité.

Par exemple, une entreprise pourra tolérer que globalement ses employés « naviguent » sur le réseau public internet par l'intermédiaire de leurs mobiles de fonction et donc autoriser les transactions entrantes et sortantes sur le port 80 traditionnellement réservé aux échanges selon le protocole HTTP (« HyperText Transfer protocol »). Elle pourra explicitement interdire l'accès à certains sites contraires à son éthique par l'intermédiaire de règles de sécurité si elle le souhaite. Elle pourra par ailleurs, en contrôlant le port 25 dédié au protocole SMTP (« Simple Mail Transfer protocol ») pour les deux sessions de communications, autoriser l'envoi et la réception de courriels vers ou en provenance de l'Intranet et refuser l'envoi et/ou la réception de courriels vers ou en provenance de l'internet.

Chaque tâche logicielle de sécurité 28, 29, est donc propre à contrôler et notamment limiter les flux de données échangés par la station mobile 21 relativement à l'un quelconque des paramètres attachés au contexte 26, 27 auquel elle est associée, et notamment un des paramètres constitutif dudit contexte 26, 27, comme par exemple pour le cas d'un contexte PDP représenté sur la figure 2, l'adresse (PDP) de la station mobile 21, la qualité de service associée à la communication, ou l'APN. Le contrôle des flux peut aussi s'effectuer à l'échelle plus globale du contexte 26, 27 en lui-même, par exemple par le biais d'un identifiant de contexte 26, 27. Cela permet d'exercer un contrôle sur l'ensemble des flux échangés dans le cadre d'une session organisée selon un contexte 26, 27 sur la base de son identifiant, à l'inverse des flux échangés dans le cadre d'une session organisée selon un autre contexte 26, 27 pour lequel on choisira de ne pas effectuer de contrôle.

Deux tâches logicielles applicatives 30, 31 - l'une traitant du transfert de fichiers selon le protocole FTP, et l'autre traitant de la consultation de pages web - échangent des données – dont le chemin logique est représenté en

pointillés sur la figure - avec des entités correspondantes dans les réseaux fixes 24, 25 par le biais des contextes 26, 27 actifs.

L'organisation des fonctions remplies par les tâches logicielles de sécurité 28, 29 utilisées dans la station mobile 21 peut correspondre à la structure des pare-feux décrite précédemment et illustrée à la figure 1. On peut aussi envisager dans le cadre de l'invention une organisation plus légère, c'est-à-dire n'incorporant que des filtres, voire même un seul filtre. La fonction de sécurité peut en outre être alors configurée de sorte que chaque filtre opère de manière unidirectionnelle, ou bidirectionnelle. L'invention n'est en effet pas limitée à une organisation spécifique de la fonction de sécurité.

La figure 3 illustre un exemple d'architecture d'un module selon l'invention. Le module 28 de sécurité comprend un module 6 de configuration relié à une mémoire 47 pour mémoriser les paramètres de sécurité associés à différents contextes PDP. Le module 28 fournit une fonction de sécurité activée par le biais de l'instanciation d'une tâche logicielle offrant les fonctions de filtrage 1, 2 et de contrôle 3 précédemment décrites sous le contrôle d'un organe 48, typiquement constitué par un processeur.

Le contrôleur 48 pilote d'autre part un ensemble 46 de contextes PDP. Il procède à l'activation d'un contexte, à la gestion des contextes actifs, et à leur fermeture le cas échéant. L'ensemble 46 consiste par exemple en une mémoire dans laquelle sont conservés les différents paramètres de chaque contexte PDP propre à l'usager utilisant le module selon l'invention. Selon l'invention, lors de l'activation d'un contexte PDP, le contrôleur 48 pilote en outre le module 28 afin de créer une instance de tâche logicielle de sécurité opérant selon les paramètres associés au contexte dont on a requis l'activation. Les valeurs de ces paramètres sont configurées au préalable et consignées dans la mémoire 47. La tâche logicielle de sécurité ainsi créée est supprimée lors de la fermeture du contexte PDP dont l'activation a donné lieu à sa création.

Dans un mode supplémentaire de réalisation de l'invention, le module 6 de configuration du pare-feu peut être agencé de manière à ce que

l'ensemble ou une portion des paramètres consignés dans la mémoire 47 soient accessibles en configuration à l'usager. Pour ce faire, le module 6 coopère avec l'application interface homme-machine du terminal de l'usager par le biais du contrôleur 48. Avantageusement, on pourra prévoir d'offrir cette option de configuration à l'usager sur une interface graphique (GUI) (« Graphical User Interface »).

L'usager peut ainsi configurer les paramètres de l'instance de tâche logicielle de sécurité qui sera créée suite à l'activation d'un contexte PDP donné. On peut aussi envisager la possibilité de définir des jeux de paramètres de tâche logicielle de sécurité associés avec un type de réseau (Réseau public, réseau privé par exemple) avec lequel l'usager est susceptible d'échanger des données.

L'invention prévoit donc la possibilité de définir des jeux de paramètres, mémorisés en mémoire 47, par le biais d'une interface graphique (GUI). Par définition d'un jeu de paramètres disponibles en configuration pour la tâche logicielle de sécurité, on entend la possibilité pour l'usager de sélectionner le ou les paramètres qu'il souhaite configurer, et d'attribuer les valeurs souhaitées aux paramètres choisis. Une interface graphique lui permettra aisément de créer, de modifier ou de supprimer des profils de sécurité associés à des contextes de session de communication.

Dans un autre mode de réalisation, l'invention est mise en œuvre au sein d'un équipement d'infrastructure d'un réseau de radiocommunication. L'invention permet alors par exemple d'effectuer un filtrage des flux échangés par contexte de session de communication relativement aux attributs de l'usager de souscription. Cela se traduit, pour un opérateur, par la possibilité de mettre en œuvre par exemple un filtre à courrier électronique commercial non sollicité (en anglais « spam ») ou un filtre à virus pour ses usagers privilégiés, sans nécessairement offrir ce service aux autres usagers. Dans le cadre des réseaux de radiocommunication GPRS ou UMTS, les contextes de session de communication sont des contextes PDP. Dans l'exemple représenté sur la figure 2, l'infrastructure de réseau de radiocommunication comprend le réseau

d'accès radio 22 et le cœur de réseau 23. La mise en œuvre de l'invention au sein d'un commutateur GGSN du cœur de réseau, par exemple, se révèle particulièrement avantageuse. D'une part, parce qu'un GGSN (de même qu'un SGSN) a la connaissance de contextes PDP actifs. Il conserve en effet une table de contextes PDP, utilisée notamment dans la gestion de la facturation. On pourra, pour plus de détails, se reporter à la description des procédures d'activation, de modification et de désactivation des contextes PDP aux paragraphes 9.2.2, 9.2.3 et 9.2.4 de la spécification 3GPP TS 23.060, version 5.6.0. On peut donc adjoindre à un GGSN un module de communication selon l'invention. D'autre part, parce que le GGSN, servant de passerelle en bordure du cœur de réseau, est un point d'ancrage des communications vu du PLMN. Il n'y a pas de transfert de GGSN au cours d'une session de communication, de sorte qu'il s'avère plus efficace d'exercer le contrôle des flux de données selon l'invention à partir de ce nœud du cœur de réseau.

Il est entendu que le module selon l'invention, dans ses différents modes de réalisation, peut être implémenté de différentes manières, comme par exemple sur une carte électronique destinée à être embarquée dans un équipement terminal de radiocommunication ou un équipement d'infrastructure de radiocommunication, ou bien sur une produit semi-conducteur, comme un ASIC (« Application Specific Integration Circuit »), sans enlever de généralité à l'invention.

REVENDICATIONS

1. Module de communication comprenant des moyens pour échanger des flux de données avec un réseau de communication dans le cadre de sessions de communication établies et organisées selon des contextes (26, 27) de session de communication, et des moyens (28, 29) de sécurité pour contrôler les flux de données échangés, caractérisé en ce que lesdits moyens (28, 29) de sécurité pour contrôler les flux de données échangés sont agencés pour opérer relativement à au moins un paramètre attaché au contexte (26, 27) de session de communication de la session correspondante.

2. Module selon la revendication 1, dans lequel les moyens (28, 29) de sécurité pour contrôler les flux de données échangés sont agencés pour opérer relativement à un identifiant du contexte (26, 27) de session de communication de la session correspondante.

3. Module selon la revendication 1, dans lequel les moyens (28, 29) de sécurité pour contrôler les flux de données échangés sont agencés pour opérer relativement à au moins un paramètre constitutif du contexte (26, 27) de session de communication de la session correspondante.

4. Module selon la revendication 3, dans lequel ledit paramètre est une adresse du module ou d'un équipement au sein duquel il est incorporé, une qualité de service associée à l'échange de flux de données, ou bien l'identifiant d'un réseau cible.

5. Module selon l'une quelconque des revendications précédentes, dans lequel les moyens pour échanger des flux de données comprennent des moyens pour échanger des flux de données en paquets, et les moyens de sécurité pour contrôler les flux de données sont agencés pour opérer sur des données en paquets.

6. Module selon l'une quelconque des revendications précédentes, dans lequel les moyens (28, 29) de sécurité pour contrôler les flux de données échangés comprennent un filtre (1, 2) pour opérer par filtrage des flux de données.

7. Module selon l'une quelconque des revendications précédentes, dans lequel les moyens (28, 29) de sécurité pour contrôler les flux de données échangés comprennent un premier et un second filtres (1, 2) pour opérer par filtrage des flux de données échangés, et une ou plusieurs passerelles (3) pour contrôler les flux de données échangées relativement à un ou plusieurs critères relatifs à une application donnée, et dans lequel l'un au moins des premier et second filtres est agencé pour opérer relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

8. Module de radiocommunication comprenant un module de communication selon l'une quelconque des revendications précédentes.

9. Station mobile (21) apte à échanger des données avec un réseau de radiocommunication (22, 23), comprenant un module de radiocommunication selon la revendication 8.

10. Equipement d'infrastructure d'un réseau de radiocommunication comprenant un module de communication selon l'une quelconque des revendications 1 à 7.

11. Procédé pour effectuer un contrôle de sécurité des flux de données échangés entre un module de communication et un réseau de communication dans des sessions de communication organisées selon des contextes de session de communication, dans lequel

- on établit une session de communication avec un correspondant distant, suivant un contexte de session de communication actif, et

- on contrôle, à l'intérieur de la session établie, les flux de données échangées selon le contexte de session de communication actif, relativement à au moins un paramètre attaché audit contexte.

12. Procédé selon la revendication 11, dans lequel on contrôle les flux de données échangées selon le contexte de session de communication actif, relativement à un identifiant dudit contexte actif.

13. Procédé selon la revendication 11, dans lequel on contrôle les flux de données échangées selon le contexte de session de communication actif, relativement à au moins un paramètre constitutif dudit contexte (26, 27) actif.

14. Procédé selon la revendication 13, dans lequel ledit paramètre est une adresse du module, une qualité de service associée à l'échange de flux de données, ou bien l'identifiant d'un réseau cible.

15. Procédé selon l'une quelconque des revendications 11 à 14, dans lequel on contrôle des flux de données en paquets, échangées selon le contexte de session de communication actif, relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

16. Procédé selon l'une quelconque des revendications 11 à 15, dans lequel on contrôle les flux de données échangées selon le contexte de session de communication actif en filtrant lesdits flux de données au moyen d'un filtre qui opère relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

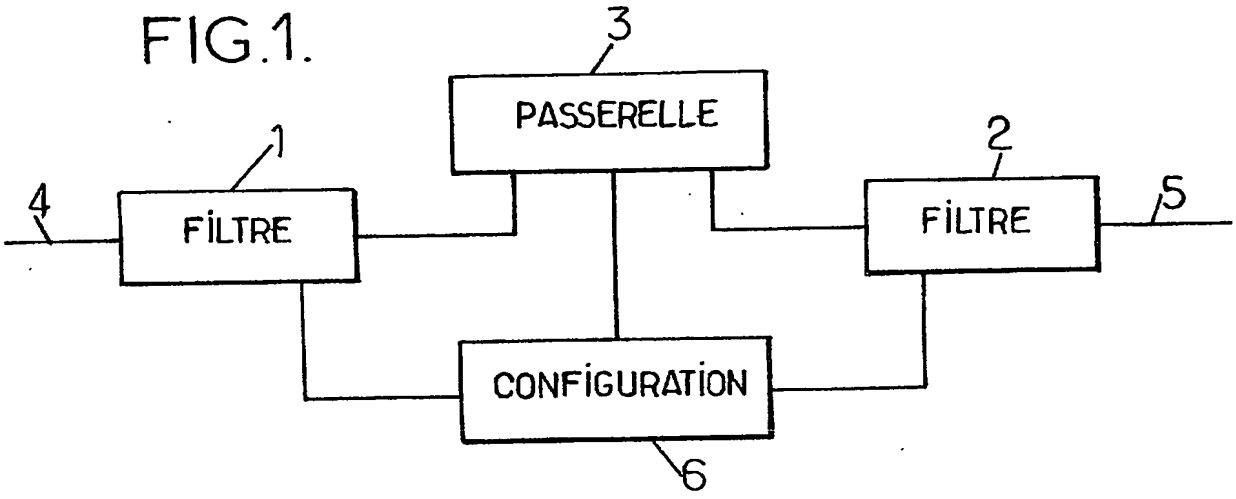
17. Procédé selon l'une quelconque des revendications 11 à 15, dans lequel on contrôle les flux de données échangées selon le contexte de session de communication actif en filtrant lesdits flux de données au moyen d'un premier et d'un second filtres pour filtrer les flux de données échangés, et d'une ou plusieurs passerelles pour contrôler les flux de données échangées relativement à un ou plusieurs critères relatifs à une application donnée, l'un au

moins des premier et second filtres étant agencé pour opérer relativement à au moins un paramètre attaché au contexte de session de communication de la session correspondante.

18. Programme d'ordinateur, chargeable dans une mémoire associée à un processeur, et comprenant des instructions pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 11 à 17 lors de l'exécution dudit programme par le processeur.

19. Support informatique sur lequel est enregistré un programme selon la revendication 18.

FIG.1.


3
PASSERELLE
1
2
4
FILTRE
FILTRE
5
CONFIGURATION
6

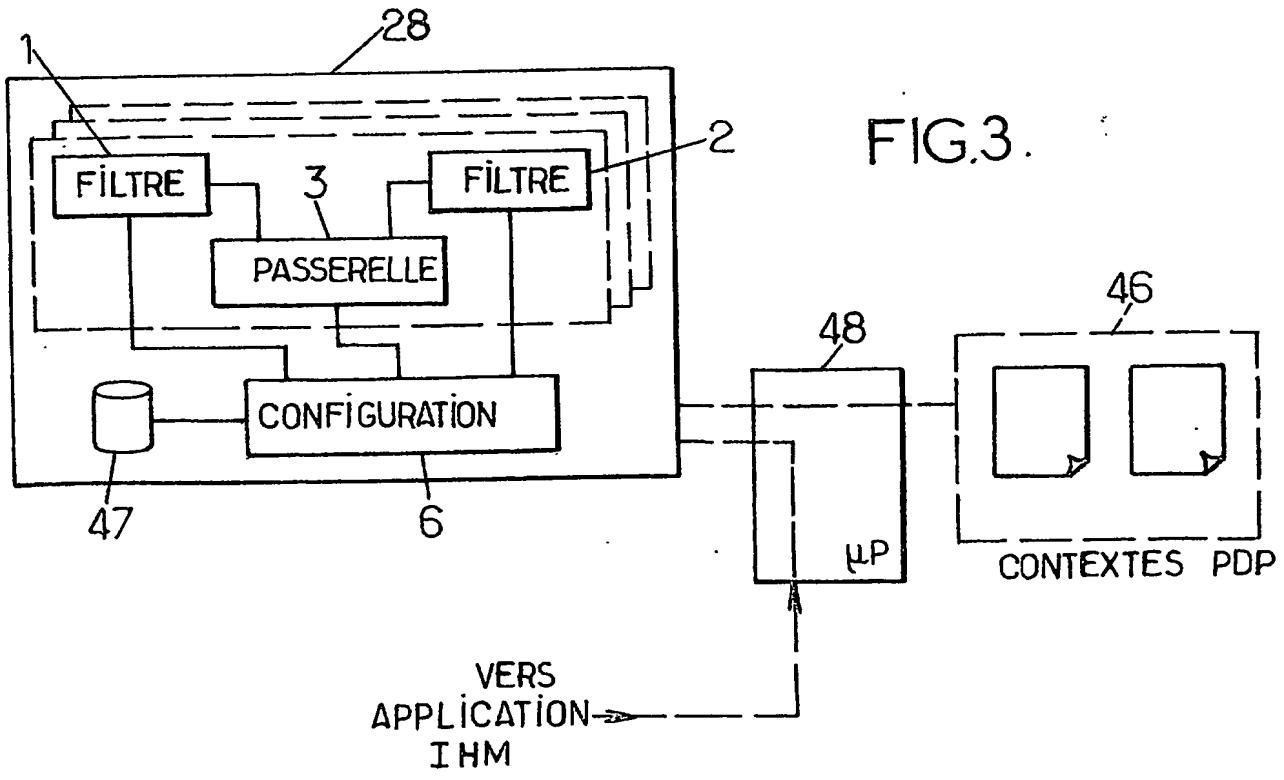
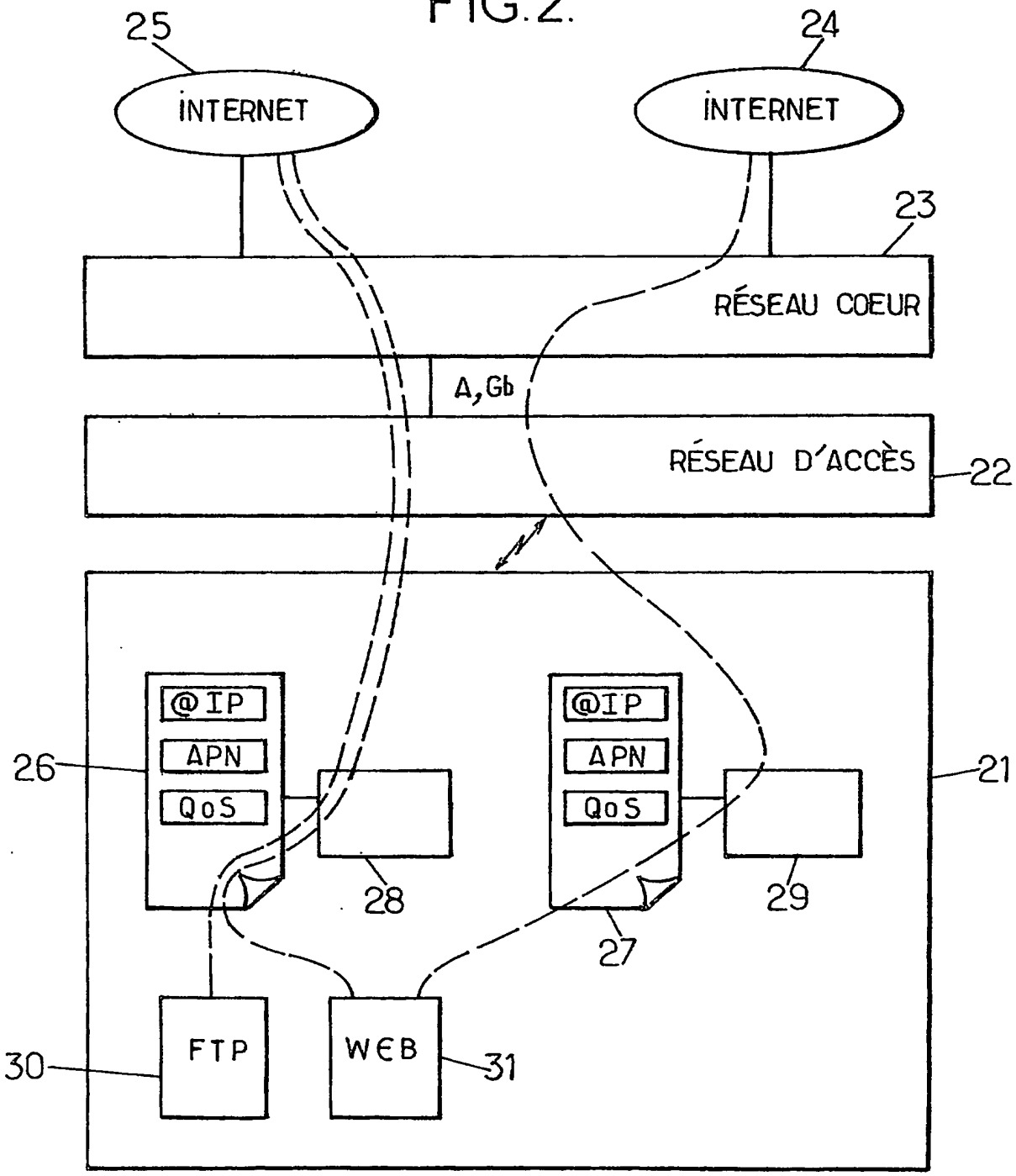

28
1
FILTRE
3
FILTRE
2
PASSERELLE
CONFIGURATION
47
6
48
46
µP
CONTEXTES PDP
VERS
APPLICATION
IHM

FIG.3.

FIG.2.


25
INTERNET
24
INTERNET
23
RÉSEAU COEUR
A,Gb
RÉSEAU D'ACCÈS
22
@IP
APN
QoS
26
@IP
APN
QoS
21
28
29
27
FTP
WEB
30
31

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1/1
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire — DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	BLO/FC-BFF030417
N° D'ENREGISTREMENT NATIONAL	

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE POUR EFFECTUER UN CONTROLE DE SECURITE DES FLUX DE DONNEES ECHANGEES ENTRE UN MODULE ET UN RESEAU DE COMMUNICATION, ET MODULE DE COMMUNICATION

LE(S) DEMANDEUR(S) :

NORTEL NETWORKS LIMITED

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		LESCUYER Pierre
Prénoms		
Adresse	Rue	31, rue Sourderie 78180 MONTIGNY-LE-BRETONNEUX FRANCE
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		LUCIDARME Thierry
Prénoms		
Adresse	Rue	1, allée Etienne Falconnet 78180 MONTIGNY-LE-BRETONNEUX FRANCE
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)	Le 20 novembre 2003 **CABINET PLASSERAUD** Bertrand LOISEL CPI n° 940311

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.